4/17/2012

Cloud Defense

Kevin Hall

Cyber Security Technology Department

Sandia National Laboratories

SAND 2012-2581C

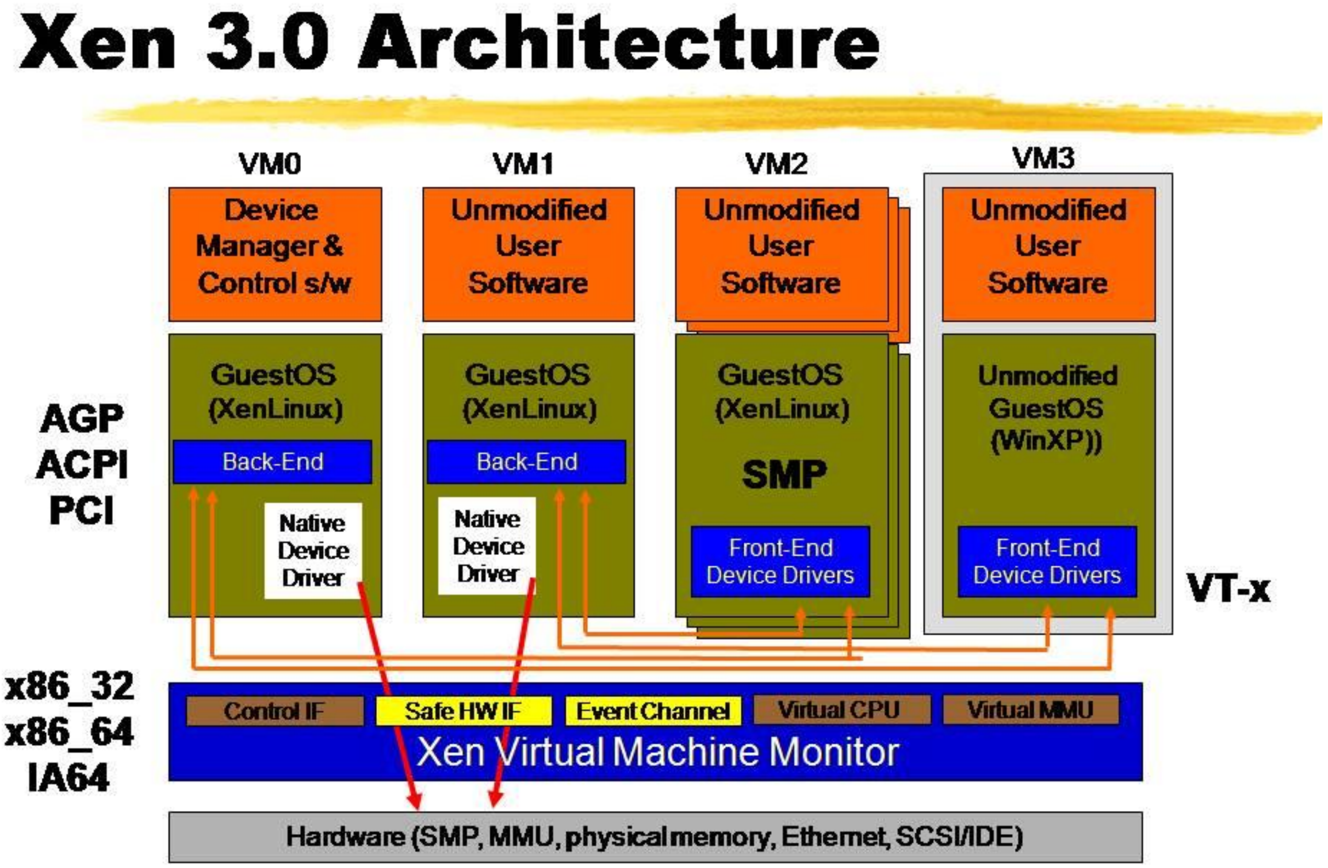
Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-0439P

.

Our environments

- Mamma cloud defense
  - Malware Analysis Multiple Memory Analytics
- Open Stack
- VMware ESX
- Windows Server 8

XEN Overview



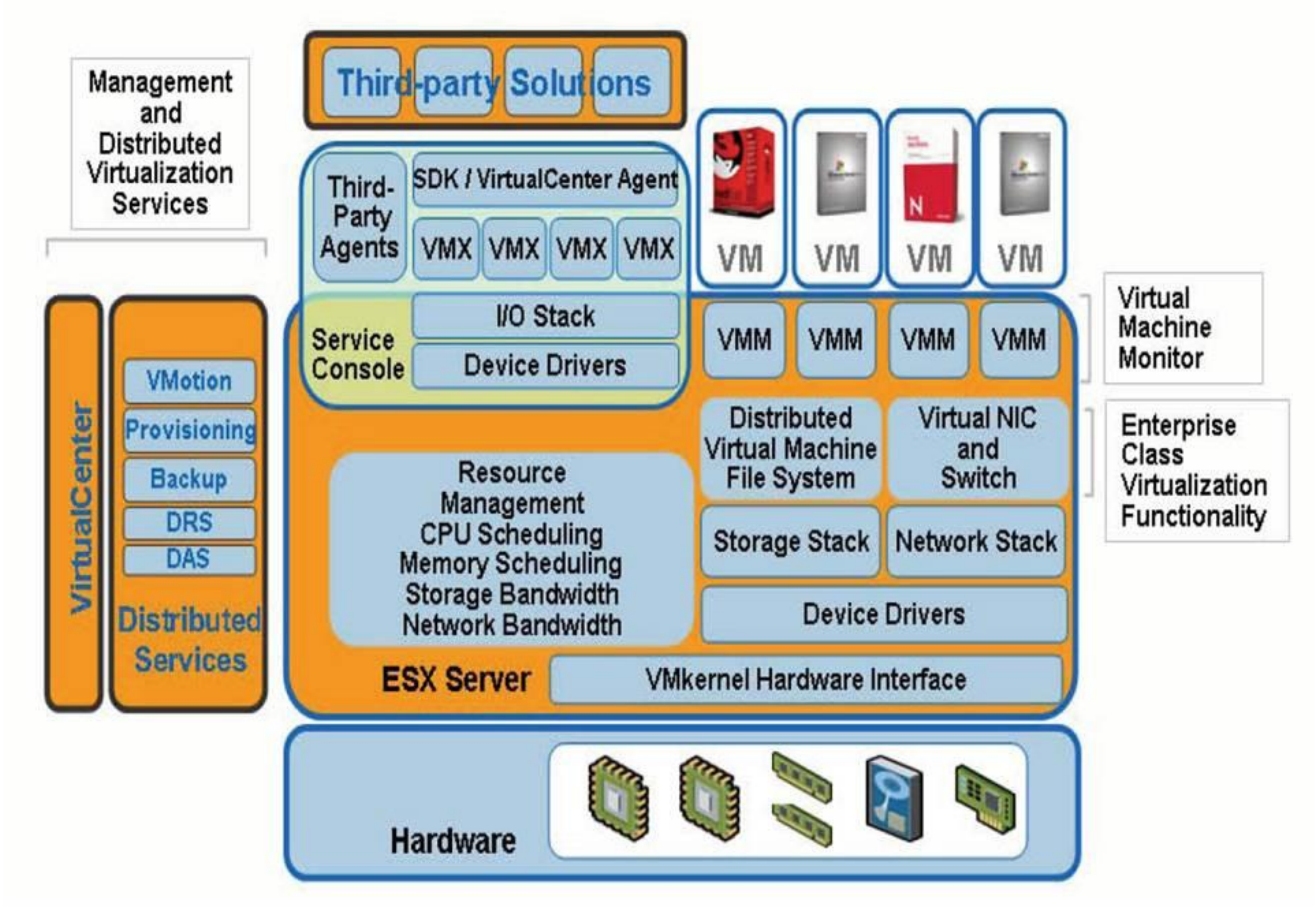
What is Open Stack

- OpenStack offers open source software to build public and private clouds.
- OpenStack is a community and a project as well as a stack of open source software to help organizations run clouds for virtual computing or storage.
- OpenStack contains a collection of open source projects that are community-maintained including OpenStack Compute (code-named Nova), OpenStack Object Storage (code-named Swift), and OpenStack Imaging Service (code-named Glance). OpenStack provides an operating platform, for orchestrating clouds.
- **http://docs.openstack.org/bexar/openstack-compute/admin/content/ch01s01.html**

Open Stack

- Open source to level the playing field so we can get a peer review of solutions.
- We can choose to share with anyone or collaborate in a university environment if desired.
- We use Open VPN or Cheap Hardware to allow connectivity Cisco ASA hardware based VPN.
- This environment can be directly hosted in Amazon cloud service. Cloud options Amazon’s EC2
- Mainly Unix based hosts and servers.
- We use GIT to hold the users profiles and settings.
- Most of this is running on 3 year old hardware.

VMware ESXi overview



VMware ESXi

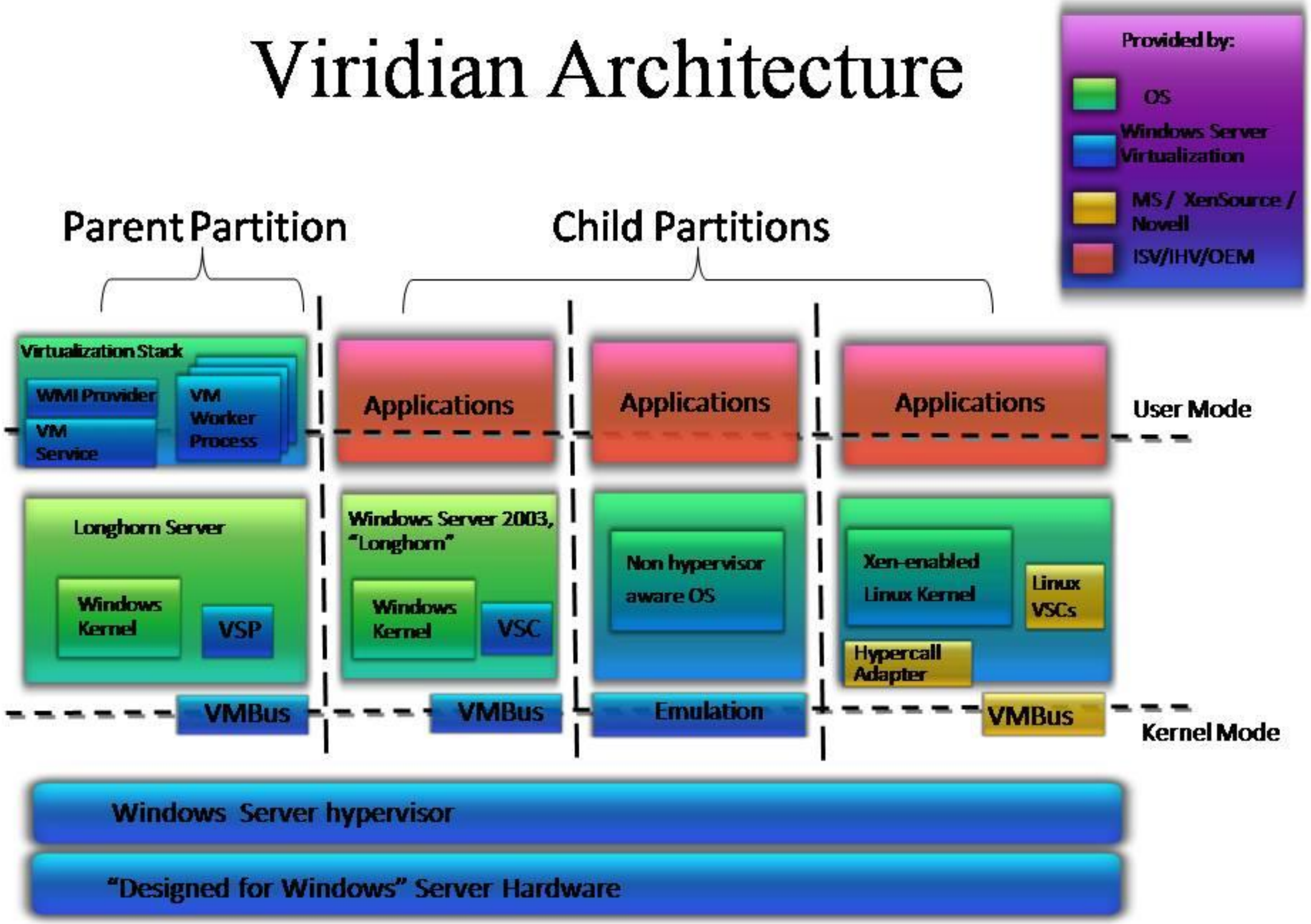
- **Learn About ESXi — VMware's Most Advanced Hypervisor Architecture**
- Like its predecessor ESX, ESXi is a "bare-metal" hypervisor, meaning it installs directly on top of the physical server and partitions it into multiple virtual machines that can run simultaneously, sharing the physical resources of the underlying server. VMware introduced ESXi in 2007 to deliver industry-leading performance and scalability while setting a new bar for reliability, security and hypervisor management efficiency.

- **http://www.vmware.com/products/vsphere/esxi-and-esx/index.html**

VMware ESX

- Internal cloud option to use for development of new tools and tactics.
- More closed and more expensive to operate however the oldest, enterprise grade, and most well understood virtual environments.
- We have tools to instrument at every level of this type of cloud hosting solution. We can perform active and passive monitoring from the hypervisor, to the hosted OS, to application stack.
- Most cloud hosting services can accept VM's from this type of private cloud virtual solution.
- Orchestra to provision and interact with hosts.
- Mainly Windows hosts in this environment.

Hyper-V overview



VSP = Virtualization Service Providers
VSC = Virtualization Service Clients

Windows Server 8

- Windows Server® is the leading server operating system that powers many of the worlds' largest datacenters, enables small businesses around the world, and delivers value to organizations of all sizes in between. Building on this legacy, Windows Server "8" delivers hundreds of new features and enhancements for transforming virtualization and cloud computing to help you reduce IT costs and deliver more business value. Within Windows Server "8" you will find exciting innovations in areas of virtualization, networking, storage, user experience, and a transition to Windows PowerShell® to take scripting to a whole new level.
- **http://www.microsoft.com/en-us/server-cloud/windows-server/v8-default.aspx**

Windows Server 8

- Very Beta at this Stage
- We are using Windows Server 8 Hyper-V
- We are developing memory and Kernel analytics
- Most of the work is in the early stage
- Expectation is to try to get ahead of the curve all of the work is 64 bit and back port to 32 bit

Private cloud testing

- Establish a VPN inside the restricted network
  - Verify and understand failure states of VPN
- Image Physical systems create Virtual systems.
- Dual home physical live systems.
- Dynamically provision systems as needed from a web front end.
- Run live malware data through sensing environment
- Capture results at every level possible
  - Splunk (Beta) hypervisor Monitor
  - Brian Payne (VMI hypervisor plugin)
  - Live memory analysis to volatility
  - WLS for the Clients OS (KCP)
- Test various memory models for sandboxing.

The Goals

- **Reduce the time to discovery for new potentially hostile binaries.**
- **Look back at past events for completeness.**
- **Flow traffic onto restricted network into the highly instrumented environment.**
- **Goal is to triage new binaries to 80% leave 20% to static.**
- **Work with IR to make sure were getting to 80%**

Leverage the VDI and Sandia in a Can

- We can use the VM templates already in place to run live fire exercises on our current environment.
- Capture metrics on what defenses are working and what isn't.

Future State

- Summer of Python and PowerShell
- Checksum internet downloaded binaries and PDF files
- Run all new (non hashed) binaries through system
- Implement a web hosting capability for others to use the testing environment for Peer Review.

Lessons Learned

kphall@sandia.gov